REMARKS

Claims 1-4, 6-9, 28 and 29 are pending in this application. By this Amendment, claim 1 is amended, claims 10-13, 15-22, and 24-27 are canceled, and claims 28 and 29 are added. Claim 1 is amended to recite that, in response to a user's request to invoke an operation of the e-commerce site, a type of user identity being used by the user is identified, where the user identity is at least one of a guest identity, a generic identity, or a registered identity, that a determination is made as to whether the type of user identity is appropriate to invoke the operation, and that, responsive to the type of user identity being appropriate to invoke the operation, a security domain is determined of the plurality of security domains to which the operation relates. Support for this amendment may be found in the current specification at least on page 11, line 26, to page 12, line 16. Support for the addition of claims 28 and 29 may be found in the current specification at least on page 11, line 26, to page 12, line 16. No new matter has been added by any of the amendments or the new claims. Reconsideration of the claims is respectfully requested in view of the following remarks.

I. Telephone Interview

Applicants thank Examiner Abedin for the courtesies extended to Applicants' representative during the July 14th, 2008 telephone interview. During the telephone interview, proposed amendments and the distinctions of the claims over the cited art were discussed. Examiner Abedin stated that he could not indicate whether the additional limitations of the proposed amendments would overcome the current rejections. However, Examiner Abedin stated he would consider the Applicants amendments and arguments one he receives the Response. The substance of the telephone interview is summarized in the following remarks.

II. 35 U.S.C. § 103, Alleged Obviousness, Claim 1-4, 6-13. 15-22, and 24-27

The Office Action rejects claims 1-4, 6-13, 15-22, and 24-27 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Wood et al. (U.S. Patent No. 6,668,322 B1) in view of Low et al. (U.S. Patent No. 6,996,605 B2) and further in view of Martherus et al. (U.S. Patent No. 7,194,764 B2). This rejection is moot with regard to canceled claims 10-13, 15-22, and 24-27 and is respectfully traversed with regard to the remaining claims.

Claim 1 reads as follows:

> 1. A method for managing multiple user identities for a user of an electronic commerce (e-commerce) site, the method comprising:
>
> defining the e-commerce site as a plurality of security domains; and
>
> in response to a user's request to invoke an operation of the e-commerce site:
>
> **identifying a type of user identity being used by the user, wherein the user identity is at least one of a guest identity, a generic identity, or a registered identity;**
>
> **determining if the type of user identity is appropriate to invoke the operation;**
>
> **responsive to the type of user identity being appropriate to invoke the operation, determining a security domain of the plurality of security domains to which the operation relates;**
>
> selecting a session from a plurality of sessions persisted for the user based on the determined security domain; and
>
> reusing the selected session for the user automatically in accordance with the determined security domain, the selected session being associated with a user identity and a role, the user identity and the role together indicating privileges for invoking operations of the e-commerce site in the determined security domain. (emphasis added)

The Office Action bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Applicant respectfully submits that Wood, Low, and Martherus, taken alone or in combination, fail to teach or provide a technical reason that, in response to a user's request to invoke an operation of the e-commerce site, a type of user identity being used by the user is identified, where the user identity is at least one of a guest identity, a generic identity, or a registered identity, that a determination is made as to whether the type of user identity is appropriate to

invoke the operation, and that, responsive to the type of user identity being appropriate to invoke the operation, a security domain is determined of the plurality of security domains to which the operation relates. Since the references fail to teach or provide a technical reason for these features, the Office Action has failed to establish a *prima facie* case of obviousness because the Office Action does not show where each and every claim limitation is taught or technically reasoned by the applied prior art.

Wood is directed to a security architecture that uses a single sign-on. In Wood, session credentials are used to maintain continuity of a persistent session across multiple accesses to one or more information resources, and in some embodiments, across credential level changes. Session credentials are secured, e.g., as a cryptographically secured session token, such that they may be inspected by a wide variety of entities or applications to verify an authenticated trust level, yet may not be prepared or altered except by a trusted authentication service.

Low is directed to a service system associated with a web site that establishes a respective communication session for selected web pages and joins to the session any party currently viewing the page. In Low, a sessions overview subsystem is notified of parties joining and leaving sessions and maintains a real-time database of current page sessions and the parties currently joined to each session. A user interface of the overview subsystem dynamically generates a session overview page from the real-time database and serves this page to a requesting permitted user, such as a customer service representative in a contact center associated with the service system. The permitted user can then select a specific session and request to be joined to it.

Martherus is directed to authenticating a user for multiple resources distributed across multiple domains through the performance of a single authentication. User access requests for a protected resource in a first domain are received and redirected to a second domain. User authentication is performed at the second domain. Martherus either transmits an authentication cookie for the second domain to the user after authentication at the second domain or redirects subsequent resource requests for resources in the first domain or a third domain to the second domain. The second domain confirms the user's authentication for applicable portions of the first, second, and third domains using the cookie.

None of the references identify **a type of user identity** being used by the user and determine if the type of user identity **is appropriate to invoke the operation**. That is, Wood merely uses a single sign-on to maintain continuity of a persistent session across multiple accesses to one or more information resources. Low merely allows a user to select a particular session from a session's overview and join the session. Martherus merely authenticates a user for multiple resources distributed across multiple domains through the performance of a single authentication much like Wood. In contradistinction, the present invention, in response to a user's request to invoke an operation of the e-commerce site, identifies a type of user identity being used by the user, then determines if the type of user identity is appropriate to invoke the operation. Responsive to the type of user identity being appropriate to invoke the operation, the present invention determines a security domain of the plurality of security domains to which the operation relates.

Furthermore, no technical rational is present in any of the references to modify the references to include such a feature. That is, there is no teaching or technical reason in Wood, Low, and Martherus, either alone or in combination, that a problem exists for which, identifying a type of user identity being used by the user, determining if the type of user identity is appropriate to invoke the operation, and, responsive to the type of user identity being appropriate to invoke the operation, determining a security domain of the plurality of security domains to which the operation relates, is a solution. To the contrary, Wood merely uses a single sign-on to maintain continuity of a persistent session across multiple accesses to one or more information resources, Low merely allows a user to select a particular session from a session's overview and join the session, and Martherus merely authenticates a user for multiple resources distributed across multiple domains through the performance of a single authentication. None of the references teaches or provide a technical reason for identifying a type of user identity being used by the user and determining if the type of user identity is appropriate to invoke the operation.

Moreover, none of the references teaches or provides a technical rational for the desirability of incorporating the subject matter of the other reference. That is, there is no motivation offered in either reference for the alleged combination. The Office Action alleges that the motivation would be "to design a method further comprising the step of selecting a session from a plurality of sessions persisted for the user based on the

determined security domain in order to provide user with multiple session access." The present invention provides for identifying a type of user identity being used by the user and determining if the type of user identity is appropriate to invoke the operation. As discussed above, none of the references teach or provides a technical reason for these features. Thus, the only teaching or technical reason to even attempt the alleged combination is based on a prior knowledge of Applicant's claimed invention thereby constituting impermissible hindsight reconstruction using Applicant's own disclosure as a guide.

One of ordinary skill in the art, being presented only with Wood, Low, and Martherus, and without having a prior knowledge of Applicant's claimed invention, would not have found it obvious to combine and modify Wood, Low, and Martherus to arrive at Applicant's claimed invention, as recited in claim 1. To the contrary, even if one were somehow motivated to combine Wood, Low, and Martherus, and it were somehow possible to combine the systems, the result would not be the invention as recited in claim 1. The resulting system would merely authenticate a user across multiple sessions using a single sign on. The resulting system would still fail to identify the type of user identity being used by the user, determine if the type of user identity is appropriate to invoke the operation, and, responsive to the type of user identity being appropriate to invoke the operation, determine a security domain of the plurality of security domains to which the operation relates.

In view of the above, Applicant respectfully submits that Wood, Low, and Martherus, taken alone or in combination, fail to teach or provide a technical reason for the features of claim 1. At least by virtue of their dependency on claim 1, the features of dependent claims 2-4 and 6-9 are not taught or technically reasoned by Wood, Low, and Martherus, whether taken individually or in combination. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 103(a).

III. 35 U.S.C. § 102, Alleged Anticipation, Claims 1, 10, and 19

The Office Action rejects claims 1, 10, and 19 under 35 U.S.C. § 102(e) as being allegedly anticipated by Hinton et al. (U.S. Patent No. 6,993,596 B2). This rejection is moot with regard to canceled claims 10 and 19 and is respectfully traversed with regard to the remaining claim.

Claim 1 reads as follows:

> 1. A method for managing multiple user identities for a user of an electronic commerce (e-commerce) site, the method comprising:
>
> defining the e-commerce site as a plurality of security domains; and
>
> in response to a user's request to invoke an operation of the e-commerce site:
>
> **identifying a type of user identity being used by the user, wherein the user identity is at least one of a guest identity, a generic identity, or a registered identity;**
>
> **determining if the type of user identity is appropriate to invoke the operation;**
>
> **responsive to the type of user identity being appropriate to invoke the operation, determining a security domain of the plurality of security domains to which the operation relates;**
>
> selecting a session from a plurality of sessions persisted for the user based on the determined security domain; and
>
> reusing the selected session for the user automatically in accordance with the determined security domain, the selected session being associated with a user identity and a role, the user identity and the role together indicating privileges for invoking operations of the e-commerce site in the determined security domain. (emphasis added)

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicants respectfully submit that Hinton does not identically show every element of claim 1

arranged as they are in the claims. Specifically, Hinton does not teach the elements emphasized above in claim 1.

Hinton is directed to transferring an Internet user directly to a domain within an e-community without returning to a home domain or re-authenticating. The user's home domain server prepares and forwards a home domain identity cookie (DIDC) with an enrollment request to a user's browser, with the enrollment request being redirected to an affiliated domain server in the e-community. The affiliated domain server prepares and sends an affiliated DIDC with an enrollment confirmation to the user's browser, redirecting the enrollment confirmation to the home domain server. The home domain server modifies the home DIDC to include a symbol which indicates successful enrollment at the affiliated site. The process may be repeated for a plurality of affiliated domains to achieve automatic enrollment in a portion of or in an entire e-community.

Nowhere in the Hinton reference is there a teaching to identify **a type of user identity** being used by the user and determine if the type of user identity **is appropriate to invoke the operation**. That is, Hinton merely uses a single sign-on to transfer a user directly to a domain within an e-community without returning to a home domain or re-authenticating. In contradistinction, the present invention, in response to a user's request to invoke an operation of the e-commerce site, identifies a type of user identity being used by the user, then determines if the type of user identity is appropriate to invoke the operation. Responsive to the type of user identity being appropriate to invoke the operation, the present invention determines a security domain of the plurality of security domains to which the operation relates. Hinton does not teach these features.

Therefore, Hinton does not teach each and every feature of independent claim 1 as is required under 35 U.S.C. § 102(e). Accordingly, Applicants respectfully request withdrawal of the rejection of claim 1 under 35 U.S.C. § 102(e).

Furthermore, Hinton does not teach, provide a technical reason, or give any incentive to make the needed changes to reach the presently claimed invention. Absent the Office Action pointing out some teaching or incentive to implement Hinton such that, in response to a user's request to invoke an operation of the e-commerce site, a type of user identity being used by the user is identified, where the user identity is at least one of a guest identity, a generic identity, or a registered identity, that a determination is made as

to whether the type of user identity is appropriate to invoke the operation, and that, responsive to the type of user identity being appropriate to invoke the operation, a security domain is determined of the plurality of security domains to which the operation relates, one of ordinary skill in the art would not be led to modify Hinton to reach the present invention when the reference is examined as a whole. Absent some teaching, technical reason, or incentive to modify Hinton in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

IV. New Claims

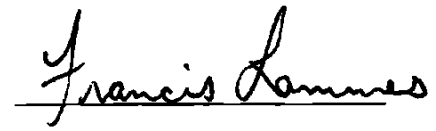
Claims 28 and 29 are added to the pending application. Support for claims 28 and 29 may be found in the current specification at least on page 11, line 26, to page 12, line 16. No new matter has been added by the addition of claims 28 and 29. Favorable consideration of claims 28 and 29 is respectfully requested.

V. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: August 4, 2008



Francis Lammes
Reg. No. 55,353
Walder Intellectual Property Law, P.C.
17330 Preston Road, Suite 100B
Dallas, TX 75252
(972) 380-9475
AGENT FOR APPLICANTS